# GSA Governmentwide
# Security Program Initiatives

ACES

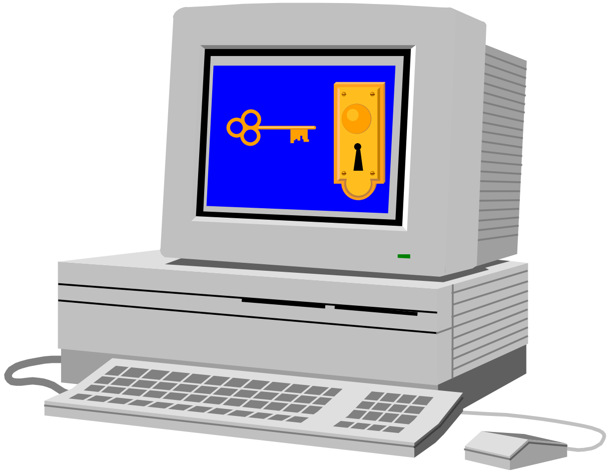
Access Certificates for Electronic Services

e-PM and Internet Security Workshop

Friday, October 22, 1999

# The Problem

The sensitivity of the data being exchanged dictates the government's diligence in ensuring the information source is legitimate, the information has not been tampered with en route, and that the transmission media is sufficiently protected.

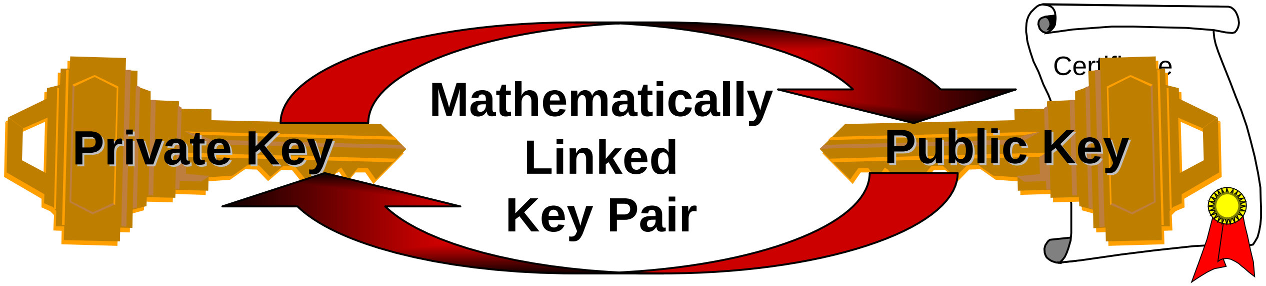


# Public Key Infrastructure

A PKI Solution offers the following features:

- Access Control
- Data Integrity
- Technical Non-Repudiation
- Confidentiality

# The Solution



Private Key

Mathematically
Linked
Key Pair

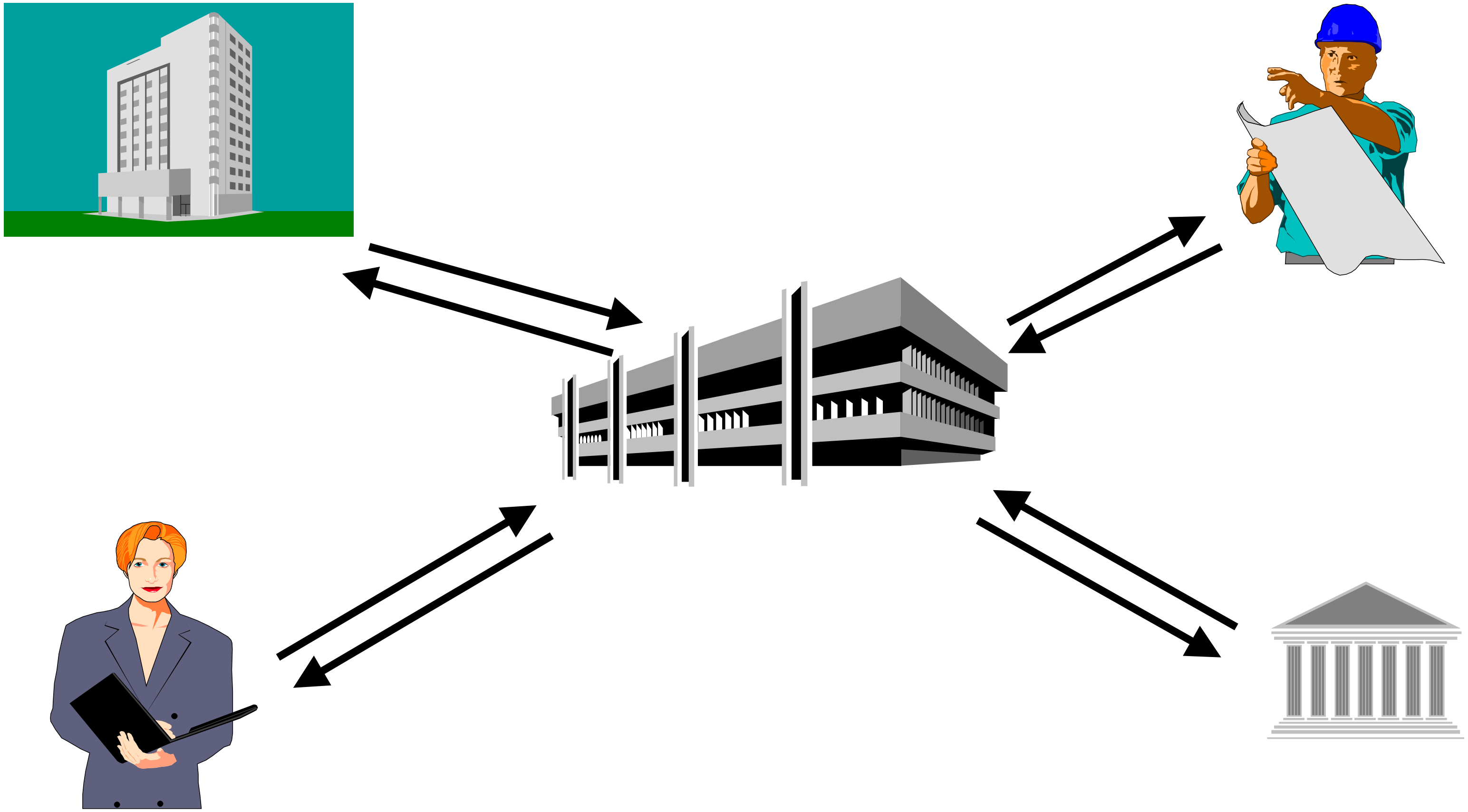
Public Key

- Protected by Owner
- Used to Sign Messages

- Distributed Openly
- Used to Verify Signatures

## Digital Signature

# The Concept



# The ACES Concept

Facilitates secure on-line access to Government information and services by the Public and Industry Partners through the use of public key technology.

# ACES Features

- Provides a Government-wide Public Key Infrastructure.
- Provides auxiliary services that participating agencies may need to make use of the Infrastructure.
- Reduces overall costs by aggregating Government requirements.

# Industry Partners

- Digital Signature Trust Company
  ABAecom, America Online, Baltimore Technologies,
  Booz Allen Hamilton, Chrysalis-ITS Luna2,
  Computer Sciences Corp. (CSC), Cygnacom Solutions,
  Entrust, ICL, Microsoft, National Computer Systems,
  National Governors Association, Netscape,
  Pricewaterhouse Coopers, Public Technology, Inc.,
  Research and Management Systems, Inc. (RAMS),
  Valicert Inc., Xcert International Inc.
- Operational Research Consultants Inc.
  Cygnacom Solutions, DataKey, Litronics, nCipher, Netscape
- AT&T
  Verisign, Inc